To provide Secure Message authentication in Wireless Sensor Network using RC6

[1]Ms. Sonam Arunsingh Bais, [2]Ms. Snehal Shrirang Mandhare
[1]Assistant Professor, [2]Assistant Professor
[1]Karmaveer Bhaurao Patil College, Vashi, India,
[2]Karmaveer Bhaurao Patil College, Vashi, India

Abstract - **Message authentication is the most efficient ways to prevent unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs). That's the reason, numerous message authentication proposals have been developed based on either symmetric-key cryptosystems or public-key cryptosystems. Many cases , have the restrictions of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. Wireless Sensor Networks (WSN) are being very popular day by day, however one of the main concern in wireless sensor network (WSN) is its limited resources.This paper the message authentication and source privacy in wireless sensor environment by using Rivest cipher version 6 (RC6) algorithm. It also compare various feature in terms of computational overhead, energy consumption, message delay, memory consumption.**

keywords - **Message authentication, Symmetric-key cryptosystem, Public-key cryptosystem, simulation, wireless sensor networks (WSNs), RC6 algorithm (Rivest cipher version 6).**

I. Introduction

In Secure transformation, Message authentication play a very important role in thwarting unauthorized ,corrupted messages from being delivered in networks to save the valuable sensor energy [8]. That’s why, Many authentication schemes have been proposed in literature to offering message authenticity & integrity verification for wireless sensor network environment (WSNs) [3]–[8]. These approaches are separated into two categories: public-key based approaches and symmetric-key based approaches [1]. The approach of Symmetric-key cryptography necessitates composite key management, lacks of scalability, not flexible to large numbers of node compromise attacks ,Therefore the message sender and the receiver have to share a secret key. In Cryptosystems, the shared key is managed by the sender to produce a message authentication code (MAC) for each transmitted message [8]. The process of the authenticity and the integrity of the message can only be confirmed by the node with the shared secret key, which is usually shared by a group of sensor nodes [2].

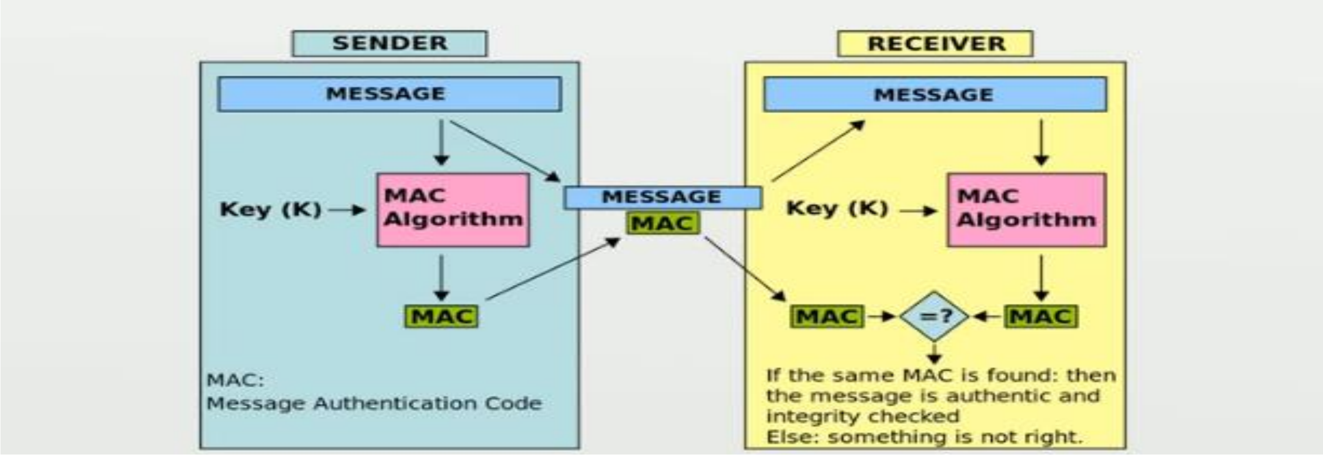

SENDER
MESSAGE
Key (K)
MAC Algorithm
MAC
MAC:
Message Authentication Code
MESSAGE
MAC
RECEIVER
MESSAGE
Key (K)
MAC Algorithm
MAC
=?
MAC
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Fig 1: message authentication code

In the public-key cryptography , Each message is transmitted along with the digital signature of the message generated using the sender’s private key. Every intermediate node forwarder and the finally receiver can authenticate the message using the sender’s public key [3]. The disadvantages of the public key based scheme is the high computational overhead . By Distinguish all the limitation and drawback over the public key cryptography, In this paper we propose the Rivest cipher version 6 algorithm for providing high security in wireless sensor environment in terms of message authentication as well as in source privacy.

II LITERATURE REVIEW

Wireless sensor networks

Wireless Sensor Network (WSN) is the collection of different sensor nodes deployed in an area to monitor the environmental and physical conditions parameters like temperature, pressure, movement of objects, light etc[6]. In a wireless sensor network sink node is known as base station. The fast development of wireless sensor networks is motivated by military applications[5]. Sensor nodes in Wireless Sensor network is very important to gather information from atmosphere and transmit it to a base station. Information sent by all the senor nodes in the network gathers at base station and from there this collected information is sent to the user through internet.

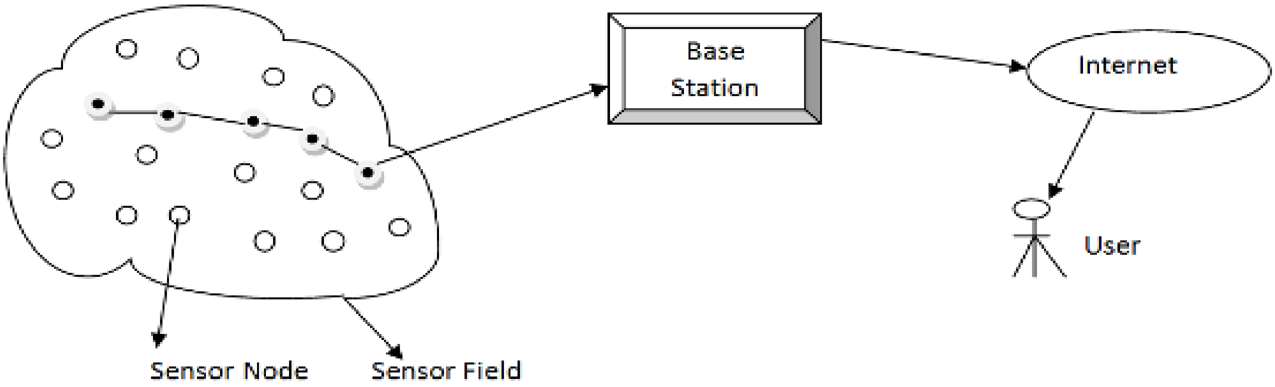


Fig 2: wireless sensor network environment

Generally, The base station is more powerful in terms of resources than the sensor nodes. The sensor node is equipped with low-power batteries due to its small sizes, Which limits the ability of the sensor node in various terms of processing, storage & transmission[8]. In this paper we propose hop by hop message authentication and source privacy using RC6 algorithm.

NS-2

Network simulation is used to simulate the networks such as in MANETs, VANETs etc. It provides simulation for routing and multicast protocols for both wired and wireless networks terminology. NS is licensed for use under version 2 of the (GNU) General Public License and is popularly known as NS2 (Network simulation version 2**).** It is an object-oriented, discrete event-driven simulator written in C++ language, Otcl/tcl. NS-2 is used to implement Network protocols as TCP and UPD, Traffic source behavior as FTP, Telnet, Web, CBR and VBR, Router queue management mechanism as Drop Tail, RED and CBQ, routing algorithms and many more. In working of ns2, C++ is used for detailed protocol implementation and Otcl is used for the setup[7].
In propose scheme we used OTcl for message authentication ,source privacy and When providing encryption and decryption by using Rivest Cipher Version 6 then C++ language is used.

III PROPOSED APPROACH

Our proposed message authentication scheme aims at achieving the following goals:

• **Message authentication**: Message authentication ensures that, The message has been sent by a genuine identity and not by a imposter[7]. The service is used provide message authentication is a **Message Authentication Code (MAC).**
• **Hop-by-hop message authentication***:* Each an every forwarder path on the routing path should be able to verify the authenticity and integrity of the messages upon recipient[1].
• **Efficiency***:* The proposed work should be efficient in terms of both computational and communication overhead[4].

Rivest Cipher 6

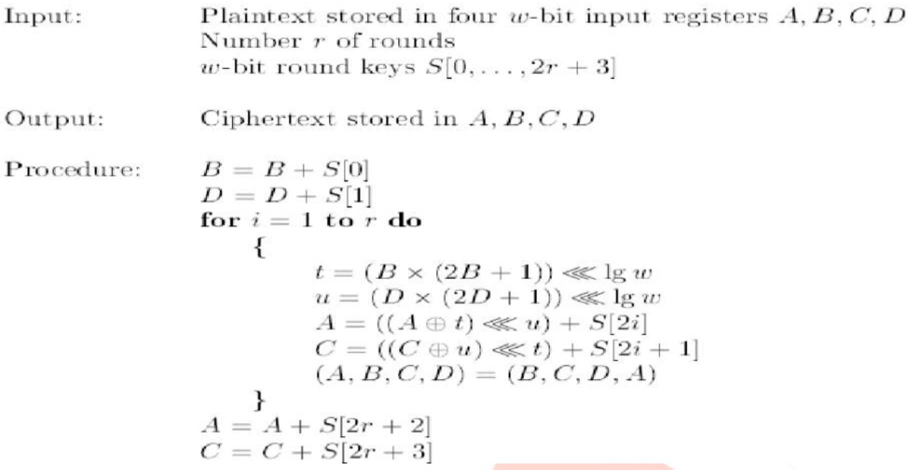
RC6 is an evolutionary improvement over RC5, Designed to meet the requirements of the Advanced Encryption Standard (AES). Like the RC5, RC6 makes essential use of data-dependent rotations. Various new features of RC6 includes the use of four working registers instead of two register, The inclusion of integer multiplication as a additional primitive operation[4]. The uses of multiplication greatly increases the diffusion achieved each round , allowing for great security, fewer rounds, and increased throughput.

Details of rc6

RC6 is a fully parameterized family of encryption algorithms. RC6 is more accurately specified as RC6=w/r/b ,Where the word size is w bits, encryption consists of a non-negative number of rounds r, and b denotes the length of the encryption key in bytes[1]. For all variants, RC6-w/r/b operates on units of four w-bit words using the following six basic operations. The base-two logarithm of w will be denoted by lgw[7].

- a + b= The integer addition modulo 2^w
- a – b = The integer subtraction modulo 2^w
- a @ b = The bitwise exclusive-or of w-bit words
- a * b = The integer multiplication modulo 2^w
- a <<< b = The rotate the w-bit word a to the left by the amount given by the least significant lgw bits of b
- a >>> b= The rotate the w-bit word a to the right by the amount given by the least significant lgw bits of b

Encryption with RC6-

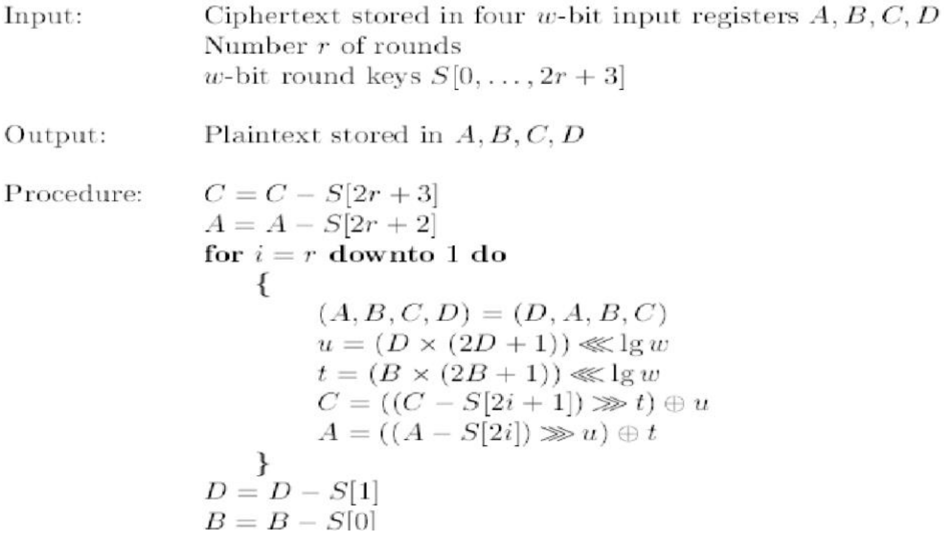


```
Input:       Plaintext stored in four $w$-bit input registers $A, B, C, D$
             Number $r$ of rounds
             $w$-bit round keys $S[0, \dots, 2r+3]$

Output:      Ciphertext stored in $A, B, C, D$

Procedure:   $B = B + S[0]$
             $D = D + S[1]$
             for $i = 1$ to $r$ do
                 {
                     $t = (B \times (2B + 1)) \lll \lg w$
                     $u = (D \times (2D + 1)) \lll \lg w$
                     $A = ((A \oplus t) \lll u) + S[2i]$
                     $C = ((C \oplus u) \lll t) + S[2i + 1]$
                     $(A, B, C, D) = (B, C, D, A)$
                 }
             $A = A + S[2r + 2]$
             $C = C + S[2r + 3]$
```

Decryption with RC6-



```
Input:       Ciphertext stored in four $w$-bit input registers $A, B, C, D$
             Number $r$ of rounds
             $w$-bit round keys $S[0, \dots, 2r+3]$

Output:      Plaintext stored in $A, B, C, D$

Procedure:   $C = C - S[2r + 3]$
             $A = A - S[2r + 2]$
             for $i = r$ downto 1 do
                 {
                     $(A, B, C, D) = (D, A, B, C)$
                     $u = (D \times (2D + 1)) \lll \lg w$
                     $t = (B \times (2B + 1)) \lll \lg w$
                     $C = ((C - S[2i + 1]) \ggg t) \oplus u$
                     $A = ((A - S[2i]) \ggg u) \oplus t$
                 }
             $D = D - S[1]$
             $B = B - S[0]$
```

IV COMPARE VARIOUS FEATURE BY USING GRAPHICAL FORMATE

Delay combime graph

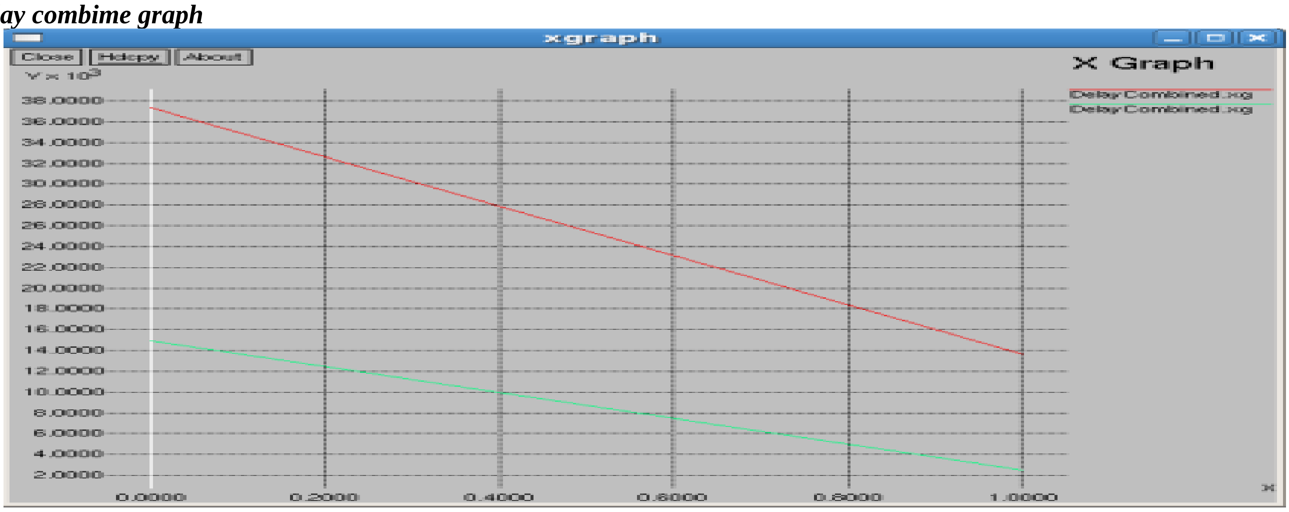


Fig 2: Number of communication verses Delay

Packet loss combine graph

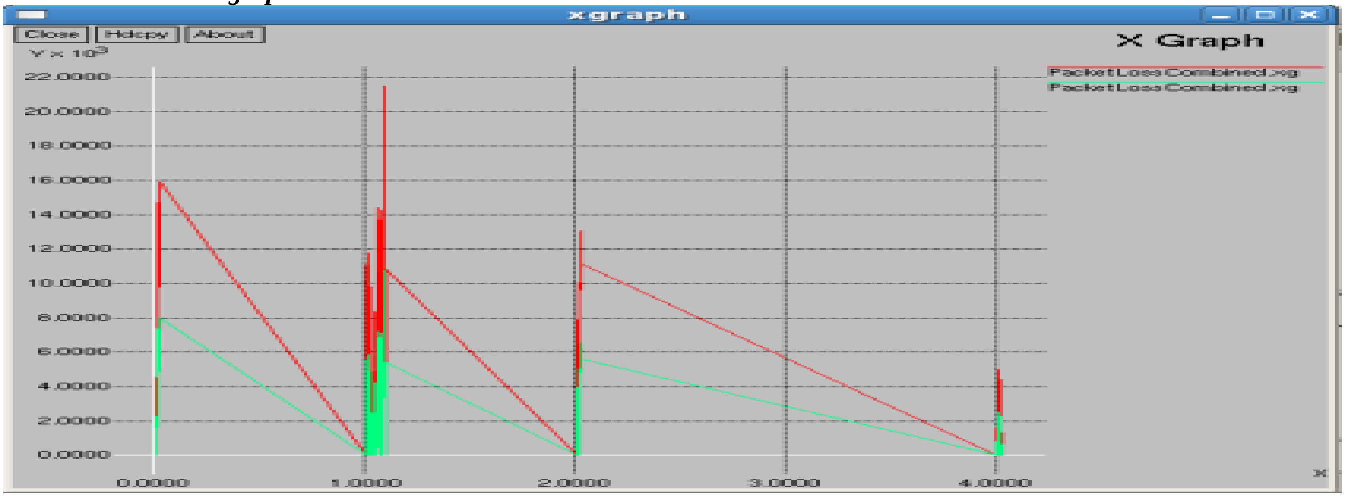


Fig 3 :Simulation time verses Packet loss

Network loss combine graph

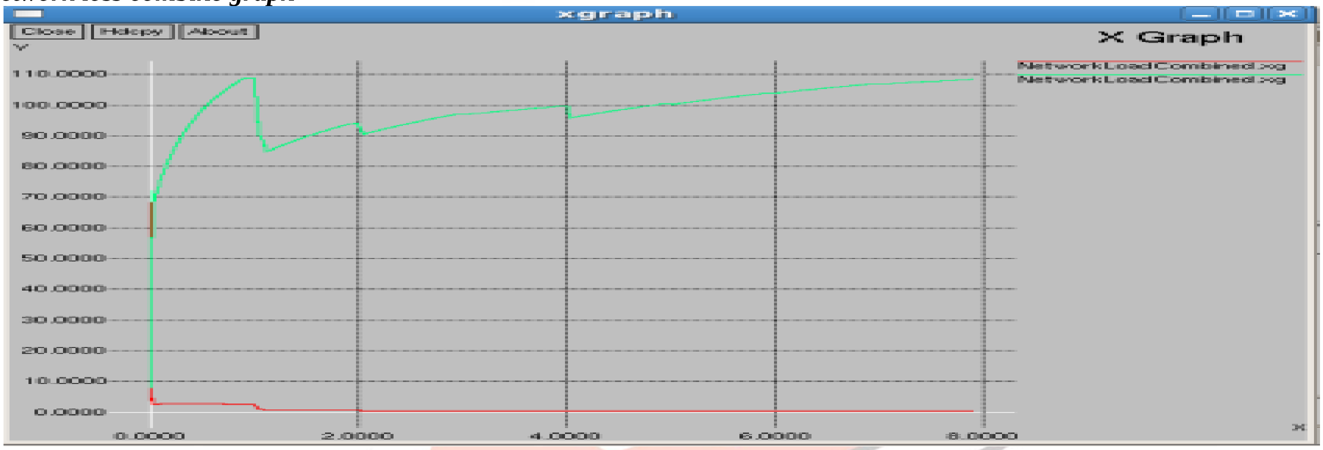


Fig 4:Simulation time verses Network loss

Cost combine graph

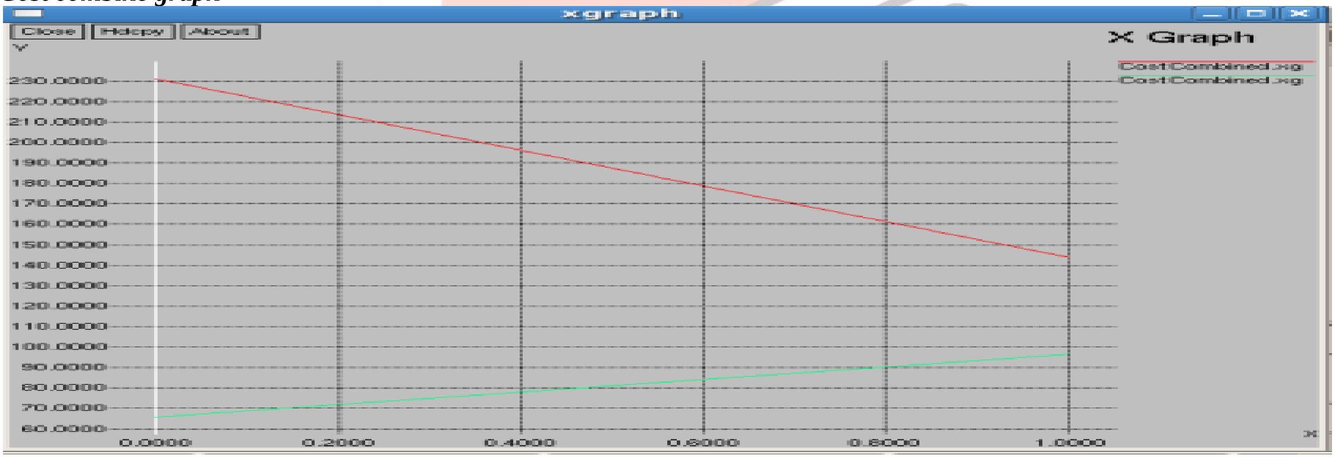


Fig 5 : Number of communication verses Cost

V ACKOWLGEMENT

To provide hop-by-hop message authentication, the disadvantages of the built in threshold of the polynomial-based scheme . We propose a hop-by-hop message authentication scheme based on the Rivest Cipher Version 6. Comparing both theoretical and simulation based results show that, Our proposed scheme is most efficient than the polynomial-based scheme in terms of Computational overhead, Energy consumption, Message delay and Memory consumption.

VI REFERENCES

[1] Jian Li Yun Li Jian Ren Jie Wu, ―Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks‖, IEEE Transactions On Parallel And Distributed Systems, pp 1-10, 2013

[2] Syed Rafiul Hussain∗ , Mitziu Echeverria† , Omar Chowdhury† , Ninghui Li, and Elisa Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information"

[3] Rekha, Kanika Wadhwa, CYBER SECURITY IN SMART GRID

[4] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, ―Attacking cryptographic schemes based on ‖perturbation polynomials‖,‖ Cryptology ePrint Archive, Report 2009/098, 2009, http://eprint.iacr.org.
[5] Dunfan Ye,DaoliGong,WeiWang ―Application of Wreless Sensor Networks in Environmental Monitoring‖, 2009 2nd International Conference on Power Electronics and Intelligent Transportation System.
[6] Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi ―Application of Wireless Sensor Networks in Energy Automation‖, Sustainable Power Generation and Supply, 2009. Supergen '09. International conference
[7] David Rojas · John Barrett "Link Quality Evaluation of a Wireless Sensor Network in Metal Marine Environments"
[8] Ian F. Akylidiz, Fellow IEEE, Tommaso Melodia, Member IEEE, and Kaushik R. Chowdhury, Student Member IEEE ―Wireless Multimedia Sensor Networks: Applications and Testbeds‖, Proceedings of the IEEE. Vol. 96, No. 10, October 2008